**1. Sample Phishing Email**

**Subject:**  
🔒 "Your PayPal Account Has Been Limited – Immediate Action Required"

**From:**  
**Email:** security@paypall.com *(note the extra “l” in "paypal")*

**Body:**

Dear Customer,

We have detected unusual activity in your PayPal account. As a precaution, your account has been temporarily limited.

**You must verify your identity to restore full access. Click the link below to proceed immediately:**

**Verify My Account**

If you do not verify within 24 hours, your account may be permanently suspended.

Thank you for your prompt attention to this matter.

Sincerely,  
PayPal Security Team

**2. Examine Sender’s Email Address for Spoofing**

* **Actual Sender:** security@paypall.com
* **Spoofed Domain:** Looks like PayPal but contains a misspelled domain (paypall.com instead of paypal.com). This is a classic spoofing method to fool users at a glance.

**3. Check Email Headers for Discrepancies**

If we analyze the email header (using MXToolbox Email Header Analyzer), we might find:

* **Return-Path:** noreply@untrusted-domain.com (doesn’t match paypal.com)
* **SPF, DKIM, DMARC:** Fails authentication checks (indicating the message likely wasn’t sent by PayPal’s servers)

**4. Identify Suspicious Links or Attachments**

* **Suspicious Link:** http://paypal.security-verify.com/login
  + Hovering reveals a mismatched domain unrelated to PayPal.
  + May lead to a credential-harvesting fake login page.

**5. Look for Urgent or Threatening Language**

* **Examples of urgency/threats:**
  + “Your account has been limited.”
  + “Immediate Action Required.”
  + “Verify within 24 hours or risk suspension.”

Phishing emails commonly use urgency to pressure the victim.

**6. Note Any Mismatched URLs**

* **Displayed URL:** Verify My Account
* **Actual URL on hover:** http://paypal.security-verify.com/login
* **Mismatch:** URL suggests PayPal but actually leads to an unrelated domain, a key sign of phishing.

**7. Verify Presence of Spelling or Grammar Errors**

* Minor issues:
  + “Click the link below to proceed immediately” is slightly unnatural.
  + “We have detected unusual activity…” is generic and lacks personalization.
  + Begins with “Dear Customer” instead of using the recipient’s name – a red flag.

**8. Summary of Phishing Traits Found**

| **Trait** | **Present?** | **Details** |
| --- | --- | --- |
| **Spoofed sender email** | ✅ | Misspelled domain paypall.com |
| **Header discrepancies** | ✅ | SPF/DKIM/DMARC failures |
| **Suspicious/malicious link** | ✅ | Hover shows misleading domain |
| **Urgent/threatening language** | ✅ | Threat of suspension in 24 hours |
| **Mismatched URLs** | ✅ | Text vs. hover mismatch |
| **Spelling/grammar issues** | ✅ | Minor errors, lack of personalization |